VIA FACSIMILE (703)872-9306

9D-HR-19614-Daum et al.
PATENT

IN THE CLAIMS

1. (withdrawn) A method for replacing an existing authentication keying variable K with a new authentication keying variable K′ generated from K, the method comprising:

generating a first authentication word, W_1, based on the existing keying variable K, a counter, C, and a master keying variable, KM;

selecting a portion of W_1 as a first portion of K′; and

completing remaining portions of K′ by iteratively:

generating new authentication words, W_n based on C, KM, and a concatenation of a prior authentication word and K; and

selecting an additional portion of W_n as an additional portion of K′.

2. (withdrawn) The method of claim 1, wherein generating new authentication words, W_n, comprises generating new authentication words based on C, KM, and a concatenation of an immediately prior authentication word W_{n-1} and K.

3. (withdrawn) The method of claim 1, wherein K′ is different in length than K.

4. (withdrawn) The method of claim 1, wherein K′ is equal in length to K.

5. (withdrawn) The method of claim 1, further comprising receiving an authentication keying variable replacement message at an appliance.

6. (withdrawn) The method of claim 1, wherein selecting a portion of W_1 comprises selecting 8-bits of W_1.

7. (withdrawn) The method of claim 6, wherein selecting a portion of W_1 comprises selecting the first 8-bits of W_1.

8. (withdrawn) The method of claim 1, wherein selecting an additional portion of W_n as an additional portion of K' comprises selecting the first 8-bits of W_n as n^{th} 8-bits of K'.

9. (withdrawn) A replacement authentication key generator comprising:

a processing circuit; and

a memory coupled to the processing circuit, the memory storing instructions for execution by the processing circuit for:

generating a first authentication word, W_1, based on the existing keying variable K, a counter, C, and a master keying variable, KM;

selecting a portion of W_1 as a first portion of K'; and

completing remaining portions of K' by iteratively:

generating new authentication words, W_n based on C, KM, and a concatenation of a prior authentication word and K; and

selecting an additional portion of W_n as an additional portion of K'.

10. (withdrawn) The replacement authentication key generator of claim 9, wherein the instructions for generating new authentication words, W_n, comprises generating new authentication words based on C, KM, and a concatenation of an immediately prior authentication word W_{n-1} and K.

11. (withdrawn) The replacement authentication key generator of claim 9, wherein K′ is different in length than K.

12. (withdrawn) The replacement authentication key generator of claim 9, wherein K′ is equal in length to K.

13. (withdrawn) The replacement authentication key generator of claim 9, wherein the instructions for selecting a portion of W_1 comprises selecting 8-bits of W_1.

14. (withdrawn) The replacement authentication key generator of claim 13, wherein the instructions for selecting a portion of W_1 comprises selecting the first 8-bits of W_1.

15. (withdrawn) The replacement authentication key generator of claim 9, wherein the instructions for selecting an additional portion of W_n as an additional portion of K′ comprises selecting the first 8-bits of W_n as n^{th} 8-bits of K′.

16. (currently amended) In an appliance communication network, a method for authenticating appliance messages, the method comprising:

maintaining at an appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance;

generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication ~~algorithm to generate a first authentication word; and~~algorithm; and

transmitting the appliance message and the first authentication word as an authenticated message to the appliance.

17. (original) The method of claim 16, further comprising:

receiving the authenticated message at the appliance;

applying the shared message counter, as stored in the appliance, and the appliance message to the authentication algorithm to generate a second authentication word; and

comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message.

18. (original) The method of claim 17, further comprising incrementing the shared message counter, as stored in the appliance, after receiving a genuine authenticated message at the appliance.

19. (original) The method of claim 16, wherein applying comprises applying an authentication keying variable, K.

20 (currently amended) The method of claim 19, wherein applying comprises:

establishing a working register R, comprising at least bytes R0, R1, R2, R3;

initializing R3 to a directional code, representing a transmission from the appliance communication center to the appliance;

initializing at least R2, R1, and R0 to the bytes C2, CI, and C0 of the shared message counter, as stored in the communication center, respectively;

iteratively ~~performing, a first number of times, the steps of:~~

~~performing~~performing at least one arithmetic, logical and shifting operation on R; and

~~shifting R; and~~

setting the first authentication word equal to the value contained in R.

21. (currently amended) The method of claim 20, wherein iteratively performing ~~a transformation of~~at least one arithmetic, logical and shifting operation on R comprises iteratively performing, as many times as there are bytes in K, the steps of:

establishing an index, equal to the greater of:

a non-zero constant; and

a number of bytes in the appliance message less one;

and

iteratively performing, a number of times equal to the index plus one:

forming P as ~~the data~~ dot product of R2 and R0;

forming Q as ~~the bitwise~~a bitwise exclusive or of P with ~~the constant~~a constant expression '01010101';

forming S by adding Q to K;

forming S' by end around rotating S;

forming T as the bitwise exclusive or of S' and R3;

forming F as the bitwise exclusive or of T with a byte of the appliance message; and

replacing R3 with R2, R2 with R1, R1 with R0, and R0 with F.

22. (original) The method of claim 21, wherein the non-zero constant is at least 3.

23. (original) The method of claim 16, wherein maintaining comprises maintaining a separate shared counter for a plurality of appliances.

24. (original) The method of claim 16, further comprising incrementing the shared message counter, as stored in the communication center, after transmitting the authenticated message to the appliance.

25. (currently amended) An appliance communication center comprising:

network connections terminating at appliances;

a processing circuit;

a memory storing a plurality of shared counters, each shared counter shared between the communication center and an appliance, the memory further storing instructions for:

maintaining at an appliance communication center a shared message counter, the shared message counter shared between the communication center and a remotely located appliance;

generating a first authentication word by applying an appliance message and the shared message counter, as stored in the communication center, to an authentication ~~algorithm to generate a first authentication word; and~~algorithm; and

transmitting the appliance message and the first authentication word as an authenticated message to the appliance.

26. (original) The appliance communication center of claim 25, wherein the instructions for maintaining comprises maintaining a separate shared counter for a plurality of appliances.

VIA FACSIMILE (703)872-9306

9D-HR-19614-Daum et al.
PATENT

27. (currently amended) The appliance communication center of claim 25, wherein the ~~instructions~~memory further ~~comprise~~stores instructions for incrementing the shared message counter, as stored in the communication center, after transmitting the authenticated message to the appliance.

28. (currently amended) In an appliance, an appliance message authentication device comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions for execution by the processor for:

~~receiving the~~receiving an authenticated message, including a first authentication word and an appliance message, at the appliance;

generating a second authentication word by applying ~~the shared~~a shared message counter, as stored in the appliance, and the appliance message ~~to the~~to an authentication ~~algorithm to generate a second authentication word; and~~algorithm; and

comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message.

29. (currently amended) The appliance message authentication device of claim 28, wherein the ~~instructions further comprise~~memory stores instructions for execution by the processor for incrementing the shared message counter, as stored in the appliance, after receiving a genuine authenticated message at the appliance.

30. (currently amended) In an appliance communication network, a method for authenticating appliance messages, the method comprising:

maintaining at an appliance a shared message counter, the shared message counter shared between the appliance and a remotely located appliance communication center;

generating a first authentication word by applying an appliance message and the shared message counter, as stored in the appliance, to an authentication ~~algorithm to generate a first authentication word; and~~algorithm; and

transmitting the appliance message and the first authentication word as an authenticated message to the appliance communication center.

31. (original) The method of claim 30, further comprising:

receiving the authenticated message at the appliance communication center;

applying the shared message counter, as stored in the appliance communication center, and the appliance message to the authentication algorithm to generate a second authentication word; and

comparing the first authentication word and the second authentication word to determine authenticity of the authenticated message.